DISA JIEO Standards Analysis **25 MAR 99**

Key Usage Extension: cRLSign bit

References:
```
X.509 section: 12.2.2.3
RFC 2459 sections: 4.2.1.3, 7.3.1, 7.3.3
FPKI Profile sections: 1.2.3, 2
MISPC section: 3.1.3.1
DII PKI Functional Specification section: 3.2.2.1.3
```

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Does the certificate issuer set cRLSign in certificates provided to the CAs that issue Certificate Revocation Lists (CRLs)?		
Does the certificate issuer set cRLSign in CA certificates only?		
If the certificate issuer sets cRLSign, does it mark the KeyUsage (KU) extension critical?		
Does the certificate user interpret the setting of KU bit 6 as cRLSign?		
Does the certificate user, only use the certified public key to validate a CA's signature on a CRL when cRLSign is set?		
If the extension is flagged critical, is the certified public key used only for verifying a signature on revocation information?		
KU keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, and decipherOnly bits are not set when the cRLSign bit is set in a CA certificate conveying a RSA public key.		
KU keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, and decipherOnly bits are not set when the cRLSign bit is set in a CA certificate conveying a DSA public key.		

Other information:

Findings:

Recommendations for Standards Work: